

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: 2003年 2月24日

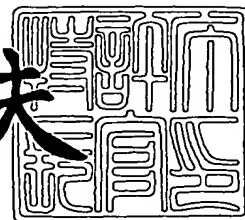
出願番号
Application Number: 特願2003-046484
[ST. 10/C]: [JP2003-046484]

出願人
Applicant(s): 松下電器産業株式会社

2003年11月20日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-3096124

【書類名】 特許願

【整理番号】 5038340101

【提出日】 平成15年 2月24日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 9/46 340

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 深井 慎一郎

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 甲斐 俊也

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 110000040

【氏名又は名称】 特許業務法人池内・佐藤アンドパートナーズ

【代表者】 池内 寛幸

【電話番号】 06-6135-6051

【手数料の表示】

【予納台帳番号】 139757

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0108331

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 プロセッサおよびこのプロセッサ用のプログラムを生成するコンパイラ装置

【特許請求の範囲】

【請求項 1】 CPUと、

プログラムを格納するための命令メモリと、

前記命令メモリに格納されているプログラムによって、動作モードを異なる動作モードへ変更する分岐命令が実行された際、分岐先アドレスに分岐許可命令が存在するか否かを判断し、前記分岐許可命令が存在する場合は動作モードの変更を許可する一方、前記分岐許可命令が存在しない場合は割り込み要求を出力する不正分岐検出部とを備えたことを特徴とするプロセッサ。

【請求項 2】 前記 CPU が実行している命令のプログラムカウンタの値によって実行領域を判定する実行領域判定部と、

前記実行領域判定部の判定結果によって、実行中の動作モードを決定する実行動作モード決定部と、

前記命令メモリに格納されているプログラムによって分岐命令が実行された際、分岐先アドレスの値によって分岐先領域を判定する分岐先領域判定部と、

前記分岐先領域判定部の判定結果によって、前記分岐命令による移行先の動作モードを決定する分岐先動作モード決定部と、

前記実行動作モード決定部によって決定された実行動作モードと、前記分岐先動作モードによって決定された移行先動作モードとを比較することによって動作モードが変更されたか否かを検出する動作モード変更検出部とをさらに備え、

前記不正分岐検出部が、前記命令メモリに格納されているプログラムによって分岐命令が実行された際、分岐先アドレスに分岐許可命令が存在しない場合は、前記動作モード変更検出部によって動作モードの変更が検出されたことを条件として前記割り込み要求を出力する、請求項 1 に記載のプロセッサ。

【請求項 3】 前記不正分岐検出部が、前記命令メモリに格納されているプログラムによって分岐命令が実行された際、分岐先アドレスに分岐許可命令が存在しない場合は、前記動作モード変更検出部によって動作モードの変更が検出され

、かつ、前記動作モード変更検出部によって検出された動作モードの変更と分岐許可命令が指定する動作モードの変更とが一致しないことを条件として、割り込み要求を出力する、請求項 2 に記載のプロセッサ。

【請求項 4】 前記分岐許可命令に、他の命令と重複しない特定の命令コードが割り当てられた、請求項 1 または 2 に記載のプロセッサ。

【請求項 5】 前記分岐許可命令に、1 つまたは複数の他の命令に対応する命令コードが重複して割り当てられた、請求項 3 に記載のプロセッサ。

【請求項 6】 分岐許可命令が検出された際、当該命令コードを他の命令に対応する命令コードに変換する分岐許可命令コード変換部をさらに備えた、請求項 3 に記載のプロセッサ。

【請求項 7】 請求項 1 ～ 6 に記載のプロセッサ用のプログラムを生成するコンパイラ装置であって、

ソースプログラムをコンパイルしアセンブラに変換する際に、ソースプログラム内の関数構造と動作モードとを判定することにより、特権領域のプログラムの所定位置に前記分岐許可命令を挿入することを特徴とするコンパイラ装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、命令メモリに対して外部からプログラムを追加できるプロセッサにおける命令実行保護に関するものである。

【0002】

【従来の技術】

通常、CPU は、命令メモリに格納されたプログラムに従って、データ処理、演算処理などの各種処理を実行する。

【0003】

以上のような従来のプロセッサについて、図面を参考にしながら以下に説明する。

【0004】

図 6 は、従来の技術によって開発されたプロセッサを用いた IC カードシステ

ムを表すブロック図である。

【0005】

従来の技術によって開発されたプロセッサを用いたICカードシステムは、図6に示すように、CPU101と、命令ROM102と、RAM103と、フラッシュメモリ104と、外部I/F105と、アンテナコイル106と、アドレスバス107aと、データバス107bと、割り込み制御回路108と、分岐許可アドレス判定回路109によって構成される。

【0006】

CPU101は、命令フェッチ部1011と、命令解読部1012と、命令実行部1013と、プログラムカウンタ1014と、メモリアクセス制御回路1015とによって構成される。

【0007】

CPU101は、命令ROM102またはフラッシュメモリ104に格納された命令を読み出し実行していく。フラッシュメモリ104に対しては、アンテナコイル106および外部I/F105を介して、外部からプログラムデータを追加することが可能である。

【0008】

図7は、従来の技術によって開発されたプロセッサを用いたメモリ空間の領域区分の概念図である。

【0009】

図7において、200は全論理アドレス空間を表す。全論理アドレス空間200は、外部I/F105、命令ROM102、RAM103、および、フラッシュメモリ104に割り当てられている。全論理アドレス空間200のうち、命令ROM空間は特権領域211とAPI領域212に、RAM領域は特権領域221とAPI領域222とユーザ領域223に、フラッシュメモリはユーザ領域に、外部I/Fはユーザ領域に、それぞれ区分されている。

【0010】

図8は、従来の技術によって開発されたプロセッサ用のプログラム概念図である。図8において、ユーザプログラム302における命令群3021は、ユーザ

プログラム 3 0 2 から特権プログラム 3 0 1 (命令群 3 0 1 1) への実行の移行を行うための処理を記述したものであり、ユーザプログラム 3 0 2 における命令群 3 0 2 2 は、ユーザプログラム 3 0 2 から特権プログラム 3 0 1 (命令群 3 0 1 2) への実行の移行を行うための処理を記述したものである。特権プログラム 3 0 1 における命令群 3 0 1 1 は、その処理内容の詳細な図示は省略してあるが、ユーザプログラム 3 0 2 から命令群 3 0 1 2 または命令群 3 0 1 3 への実行の移行を行うための処理を記述したものである。

【0 0 1 1】

従来の技術によって開発された上記 IC カードシステムにおいては、ユーザプログラムによって特権プログラムおよび API プログラムが不正に実行されることを防ぎ、セキュリティを確保するために、動作モードの移行を伴う分岐が発生した場合は、以下に示す方法がとられる(例えば特許文献 1 を参照。)。

【0 0 1 2】

第一に、ユーザプログラム上で実行を希望する特権プログラムまたは API プログラムが格納されているアドレスを、演算用レジスタに設定する。第二に、分岐許可アドレス判定回路 1 0 9 によって定められた特定の分岐許可アドレスに対して分岐命令を実行する。第三に、分岐許可アドレス上に格納されている条件判定プログラムによって、演算用レジスタに設定されたアドレスの正当性が判定され、正当であれば、ユーザプログラムが実行を希望する特権プログラムまたは API プログラムが格納されているアドレスに対し、再度分岐命令が実行される。

【0 0 1 3】

また、ユーザプログラムから、分岐許可アドレス判定回路 1 0 9 に定められていない特権プログラムまたは API プログラム中のアドレスに対して分岐命令を実行した場合は、分岐許可アドレス判定回路 1 0 9 によって割り込み要求が出力されるため、セキュリティが確保される。

【0 0 1 4】

【特許文献 1】

特開 2 0 0 2 - 1 8 2 9 3 1 号公報

【0 0 1 5】

【発明が解決しようとする課題】

しかしながら、上記のようなプロセッサを用いた I C カードシステムにおいては、ユーザプログラムから特権プログラムに実行が移行する際に条件判定プログラムの実行が発生するため、リアルタイム性が低下するという問題がある。

【0 0 1 6】

本発明は、上記従来の問題点を解決するためのものであり、ユーザプログラムから特権プログラムへ実行が移行する際のセキュリティを確保しつつ、リアルタイム性向上が可能なプロセッサを提供することを目的とする。

【0 0 1 7】**【課題を解決するための手段】**

上記の目的を達成するために、本発明のプロセッサは、C P U と、プログラムを格納するための命令メモリと、前記命令メモリに格納されているプログラムによって、動作モードを異なる動作モードへ変更する分岐命令が実行された際、分岐先アドレスに分岐許可命令が存在するか否かを判断し、前記分岐許可命令が存在する場合は動作モードの変更を許可する一方、前記分岐許可命令が存在しない場合は割り込み要求を出力する不正分岐検出部とを備えたことを特徴とする。

【0 0 1 8】**【発明の実施の形態】**

上述の構成にかかる本発明のプロセッサに関して、動作モードの変更とは、例えば、ある動作モードから、当該動作モードよりも高い権限を必要とする動作モードへの変更を言う。

【0 0 1 9】

上記の構成を備えたことにより、本発明のプロセッサは、ユーザプログラムから例えば特権プログラムまたは A P I プログラム中のアドレスに対して分岐命令が実行された際、分岐先アドレス上に分岐許可命令が格納されていない場合は不正分岐検出部が割り込み要求信号を出力するため、ユーザプログラムによって特権プログラム等が不正に実行されることを防ぎ、セキュリティを確保できる。またユーザプログラム上から、特権プログラムまたは A P I プログラムを正当に実行する際、ユーザプログラム上で実行を希望する特権プログラムまたは A P I プ

プログラムが格納されているアドレスに対して、分岐命令を直接実行することができるため、動作モードの移行に伴う処理時間が削減され、リアルタイム性が向上する。

【 0 0 2 0 】

本発明のプロセッサは、前記CPUが実行している命令のプログラムカウンタの値によって実行領域を判定する実行領域判定部と、前記実行領域判定部の判定結果によって、実行中の動作モードを決定する実行動作モード決定部と、前記命令メモリに格納されているプログラムによって分岐命令が実行された際、分岐先アドレスの値によって分岐先領域を判定する分岐先領域判定部と、前記分岐先領域判定部の判定結果によって、前記分岐命令による移行先の動作モードを決定する分岐先動作モード決定部と、前記実行動作モード決定部によって決定された実行動作モードと、前記分岐先動作モードによって決定された移行先動作モードとを比較することによって動作モードが変更されたか否かを検出する動作モード変更検出部とをさらに備え、前記不正分岐検出部が、前記命令メモリに格納されているプログラムによって分岐命令が実行された際、分岐先アドレスに分岐許可命令が存在しない場合は、前記動作モード変更検出部によって動作モードの変更が検出されたことを条件として前記割り込み要求を出力することが好ましい。

【 0 0 2 1 】

前記の構成において、分岐許可命令には、他の命令と重複しない特定の命令コードを割り当てることが好ましい。これにより、他の命令を処理するための資源に影響を与えることがなく、リアルタイム性を向上させることができる。

【 0 0 2 2 】

また、本発明のプロセッサは、前記不正分岐検出部が、前記命令メモリに格納されているプログラムによって分岐命令が実行された際、分岐先アドレスに分岐許可命令が存在しない場合は、前記動作モード変更検出部によって動作モードの変更が検出され、かつ、前記動作モード変更検出部によって検出された動作モードの変更と分岐許可命令が指定する動作モードの変更とが一致しないことを条件として、割り込み要求を出力することがさらに好ましい。また、この構成において、前記分岐許可命令には、1つまたは複数の他の命令に対応する命令コードを

重複して割り当てることが好ましい。あるいは、分岐許可命令が検出された際、当該命令コードを他の命令に対応する命令コードに変換する分岐許可命令コード変換部をさらに備えた構成とすることも好ましい。

【0023】

また、上記の目的を達成するために、本発明にかかるコンパイラ装置は、上述のいずれかの構成にかかるプロセッサ用のプログラムを生成するコンパイラ装置であって、ソースプログラムをコンパイルしアセンブラに変換する際に、ソースプログラム内の関数構造と動作モードとを判定することにより、特権領域のプログラムの所定位置に前記分岐許可命令を挿入することを特徴とする。

【0024】

以下、本発明のプロセッサおよびコンパイラ装置の具体例について、図面を参照しながら説明する。

【0025】

(実施の形態1)

本発明のプロセッサの一実施形態について、図1を参照しながら説明する。

【0026】

図1は、本実施形態のプロセッサを用いたICカードシステムを表すブロック図である。

【0027】

本実施形態のプロセッサを用いたICカードシステムは、図1に示すように、CPU401と、命令ROM402と、RAM403と、フラッシュメモリ404と、外部I/F405と、アンテナコイル406と、アドレスバス407aと、データバス407dと、割り込み制御回路408と、不正分岐検出回路409と、実行領域判定回路410と、実行動作モード決定回路411と、分岐先領域判定回路412と、分岐先動作モード決定回路413と、動作モード変更検出回路414とによって構成される。

【0028】

更に、CPU401は、命令フェッチ部4011と、命令解読部4012と、命令実行部4013と、プログラムカウンタ4014と、メモリアクセス制御回

路 4015 によって構成される。

【0029】

CPU401は、命令ROM402またはフラッシュメモリ404に格納された命令を読み出し実行していく。フラッシュメモリ404に対しては、アンテナコイル406および外部I/F405を介して、外部からプログラムデータを追加することが可能である。

【0030】

図7は、本実施形態のプロセッサを用いたメモリ空間の領域区分の概念図である。

【0031】

図7において、200は全論理アドレス空間を表し、命令ROM空間は特権領域211とAPI領域212に、RAM領域は特権領域221とAPI領域222とユーザ領域223に、フラッシュメモリはユーザ領域に、外部I/Fはユーザ領域に、それぞれ区分されている。

【0032】

図2は、本実施形態のプロセッサ用のプログラム概念図である。

【0033】

図2に示すように、特権領域中の特権プログラム501およびAPI領域中のAPIプログラム502のそれぞれには、ユーザ領域中のユーザプログラム503から、分岐命令(jmp)によって、特権領域中の特権プログラム501またはAPI領域中のAPIプログラム502に実行が移行する際に、分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令(accept)を記述する。ここで、分岐許可命令(accept)は、既存命令の命令コードと一致しない特別の命令コードを持つ。

【0034】

実行領域判定回路410は、実行プログラムカウンタ値s4018から、図7に示したメモリ空間の領域区分に従い、現在実行されている命令の領域が特権領域、API領域、ユーザ領域のいずれであることを判定する。判定結果は、実行領域判定信号s410として実行動作モード決定回路411へ出力される。実行動

作モード決定回路 4 1 1 は、実行領域判定信号 s 4 1 0 の値に従い、実行動作モードを、特権モード、A P I モード、ユーザモードのいずれかに決定する。決定結果は、実行動作モード決定信号 s 4 1 1 として出力される。

【 0 0 3 5 】

C P U 4 0 1 は、命令フェッチプログラムカウンタ値 s 4 0 1 5 または分岐先アドレス値 s 4 0 1 4 のいずれかをメモリアクセス制御回路 4 0 1 5 によって選択して、メモリアクセスアドレス信号 s 4 0 1 6 として出力する。

【 0 0 3 6 】

分岐先領域判定回路 4 1 2 は、メモリアクセスアドレス信号 s 4 0 1 6 から、図 7 に示したメモリ空間の領域区分に従い、分岐先命令の領域が特権領域、A P I 領域、ユーザ領域のいずれであるかを判定し、判定結果として分岐先領域判定信号 s 4 1 2 を出力する。分岐先動作モード決定回路 4 1 3 は、分岐先領域判定信号 s 4 1 2 の値に従い、動作モードを特権モード、A P I モード、ユーザモードのいずれかに決定し、決定結果として分岐先動作モード決定信号 s 4 1 3 を出力する。

【 0 0 3 7 】

動作モード変更検出回路 4 1 4 は、実行動作モード決定信号 s 4 1 1 と分岐先動作モード決定信号 s 4 1 3 から動作モードの変化を検出し、動作モード変化検出信号 s 4 1 4 を出力する。

【 0 0 3 8 】

不正分岐検出回路 4 0 9 は、動作モード変化検出信号 s 4 1 4 と命令フェッチデータ s 4 0 7 d とに従い、以下の処理を行う。

【 0 0 3 9 】

不正分岐検出回路 4 0 9 は、動作モード変更検出信号 s 4 1 4 によって、ユーザプログラムから A P I プログラム、または、ユーザプログラムから特権プログラムへの実行の移行を伴う分岐命令が発生したことを判定した場合は、分岐先アドレスに格納されている命令コードを解読し、ユーザプログラムからの分岐を許可する分岐許可命令 (a c c e p t) でない場合は、割り込み要求として不正分岐検出割り込み要求信号 s 4 0 9 を発生させる。

【0 0 4 0】

なお、不正分岐検出回路 4 0 9 は、動作モード変更検出信号 s 4 1 4 によって動作モードが変更しないと判定した場合、あるいは、動作モードが変更する場合であっても、その動作モードの変更が、ユーザプログラムから A P I プログラムへの変更、または、ユーザプログラムから特権プログラムへの変更のいずれでもないと判定した場合は、何も処理しない。

【0 0 4 1】

C P U 4 0 1 内部の分岐許可命令 (a c c e p t) に対する処理は、命令解読部 4 0 1 2 を機能拡張し、命令実行部 4 0 1 3 の制御をノーオペレーション命令と同一にすることで、C P U 4 0 1 内部のデータ・演算処理用の資源に影響を与えることなく、最短実行処理サイクルで実行される。

【0 0 4 2】

以上により、動作モードの移行を伴う分岐命令が実行された際、分岐先アドレス上にその分岐命令の実行を許可する分岐許可命令が格納されていない場合は、不正分岐検出回路 4 0 9 が割り込み要求信号 s 4 0 9 を出力するため、例えばフラッシュメモリ 4 0 4 に外部から追加されたユーザプログラム等によって命令 R O M 4 0 2 に格納された特権プログラムが不正に実行されることを防ぎ、セキュリティを確保できる。また、正当な処理の場合、実行を希望するプログラムが格納されているアドレスに対して直接分岐命令を実行できるので、動作モードの移行を最短実行処理サイクルで処理でき、リアルタイム性が向上する。

【0 0 4 3】

(実施の形態 2)

本発明の実施の形態 2 にかかるプロセッサを用いた I C カードシステムについて、以下に説明する。

【0 0 4 4】

本実施形態のプロセッサを用いた I C カードシステムのハードウェア構成は、実施の形態 1 の I C カードシステムと同様である (図 1 参照)。また、本実施形態のプロセッサを用いたメモリ空間の領域区分も、実施の形態 1 と同様である (図 7 参照)。

【0045】

図3は、本実施形態のプロセッサ用のプログラム概念図である。

【0046】

A P I 領域中の A P I プログラム 6 0 2 には、ユーザ領域中のユーザプログラム 6 0 3 から分岐命令 (j m p) によって A P I 領域中の A P I プログラム 6 0 2 に実行が移行する際に、A P I 領域中の分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令 (a c c e p t u s r) を記述する。

【0047】

特権領域中の特権プログラム 6 0 1 には、ユーザ領域中のユーザプログラム 6 0 3 から分岐命令 (j m p) によって特権領域中の特権プログラム 6 0 1 に実行が移行する際に、特権領域中の分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令 (a c c e p t u s r) を記述する。

【0048】

また、特権領域中の特権プログラム 6 0 1 には、A P I 領域中の A P I プログラム 6 0 2 から分岐命令 (j m p) によって特権領域中の特権プログラム 6 0 1 に実行が移行する際に、特権領域中の分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令 (a c c e p t a p i) を記述する。

【0049】

ここで、分岐許可命令 (a c c e p t) は既存命令の命令コードと一致しない特別の命令コードを持つ。

【0050】

実行領域判定回路 4 1 0 は、実行プログラムカウンタ値 s 4 0 1 8 から、図7に示したメモリ空間の領域区分に従い、現在実行されている命令の領域が特権領域、A P I 領域、ユーザ領域のいずれであるかを判定し、判定結果として実行領域判定信号 s 4 1 0 を出力する。実行動作モード決定回路 4 1 1 は、実行領域判定信号 s 4 1 0 の値に従い、実行動作モードを特権モード、A P I モード、ユーザモードのいずれかに決定する。決定結果は、実行動作モード決定信号 s 4 1 1 として出力される。

【0051】

CPU401は、命令フェッチプログラムカウンタ値s4015または分岐先アドレス値s4014いずれかをメモリアクセス制御回路4015によって選択し、メモリアクセスアドレス信号s4016として出力する。

【0052】

分岐先領域判定回路412は、メモリアクセスアドレス信号s4016から、図7に示したメモリ空間の領域区分に従い、分岐先命令の領域が特権領域、API領域、ユーザ領域のいずれであるかを判定し、判定結果として分岐先領域判定信号s412を出力する。分岐先動作モード決定回路413は分岐先領域判定信号s412の値に従い動作モードを特権モード、APIモード、ユーザモードのいずれかに決定する。決定結果は、分岐先動作モード決定信号s413として出力される。

【0053】

動作モード変更検出回路414は、実行動作モード決定信号s411と分岐先動作モード決定信号s413から動作モードの変化を検出し、動作モード変更検出信号s414を出力する。

【0054】

不正分岐検出回路409は、動作モード変更検出信号s414と、命令フェッチデータs407dに従い、以下の処理を行う。

【0055】

不正分岐検出回路409は、動作モード変更検出信号s414によってユーザプログラムからAPIプログラムまたはユーザプログラムから特権プログラムへの実行の移行を伴う分岐命令が発生したことを判定した場合は、分岐先アドレスに格納されている命令コードを解読し、ユーザプログラムからの分岐を許可する分岐許可命令(accept usr)でない場合は、割り込み要求として不正分岐検出割り込み要求信号s409を発生させる。

【0056】

不正分岐検出回路409は、動作モード変更検出信号s414によってAPIプログラムから特権プログラムへの実行の移行を伴う分岐命令が発生したことを判定した場合は、分岐先アドレスに格納されている命令コードを解読し、ユーザ

プログラムからの分岐を許可する分岐許可命令 (accept usr) または API プログラムからの分岐を許可する分岐許可命令 (accept api) でない場合は、割り込み要求として不正分岐検出割り込み要求信号 s 4 0 9 を発生させる。

【0057】

不正分岐検出回路 4 0 9 は、動作モード変更検出信号 s 4 1 4 によって、動作モードが変更しないと判定した場合、あるいは、動作モードが変更する場合であっても、その動作モードの変更が、ユーザプログラムから API プログラムへの変更、ユーザプログラムから特権プログラム、または、API プログラムから特権プログラムへの変更のいずれでもないと判定した場合は、何も処理しない。

【0058】

CPU 4 0 1 内部の分岐許可命令 (accept) に対する処理は、命令解読部 4 0 1 2 を機能拡張し、命令実行部 4 0 1 3 の制御をノーオペレーション命令と同一にすることで、CPU 4 0 1 内部のデータ・演算処理用の資源に影響を与えることなく、最短実行処理サイクルで実行される。

【0059】

以上により、動作モードの移行を伴う分岐命令が実行された際、分岐先アドレス上にその分岐命令の実行を許可する分岐許可命令が格納されていない場合は、不正分岐検出回路 4 0 9 が割り込み要求信号 s 4 0 9 を出力するため、フラッシュメモリ 4 0 4 に外部から追加されたユーザプログラム等によって命令 ROM 4 0 2 に格納された特権プログラムが不正に実行されることを防ぎ、セキュリティを確保できる。正当な処理の場合、実行を希望するプログラムが格納されているアドレスに対して直接分岐命令を実行できるので、動作モードの移行を最短実行処理サイクルで処理でき、リアルタイム性が向上する。

【0060】

(実施の形態 3)

本発明の実施の形態 3 にかかるプロセッサを用いた IC カードシステムについて、以下に説明する。

【0061】

本実施形態のプロセッサを用いた I C カードシステムのハードウェア構成は、実施の形態 1 の I C カードシステムと同様である（図 1 参照）。また、本実施形態のプロセッサを用いたメモリ空間の領域区分も、実施の形態 1 と同様である（図 7 参照）。

【 0 0 6 2 】

図 3 は、本実施形態のプロセッサ用のプログラム概念図である。

【 0 0 6 3 】

A P I 領域中の A P I プログラム 6 0 2 には、ユーザ領域中のユーザプログラム 6 0 3 から分岐命令 (j m p) によって A P I 領域中の A P I プログラム 6 0 2 に実行が移行する際に、A P I 領域中の分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令 (a c c e p t u s r) を記述する。

【 0 0 6 4 】

特権領域中の特権プログラム 6 0 1 には、ユーザ領域中のユーザプログラム 6 0 3 から分岐命令 (j m p) によって特権領域中の特権プログラム 6 0 1 に実行が移行する際に、特権領域中の分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令 (a c c e p t u s r) を記述する。

【 0 0 6 5 】

また特権領域中の特権プログラム 6 0 1 には、A P I 領域中の A P I プログラム 6 0 2 から分岐命令 (j m p) によって特権領域中の特権プログラム 6 0 1 に実行が移行する際に、特権領域中の分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令 (a c c e p t a p i) を記述する。

【 0 0 6 6 】

上述のように、本実施形態のプロセッサ用のプログラム記述方法は、実施の形態 2 と同じである。しかし、本実施形態のプロセッサは、ユーザプログラムからの分岐を許可する分岐許可命令 (a c c e p t u s r) および A P I プログラムからの分岐を許可する分岐許可命令 (a c c e p t a p i) に、それぞれ特殊な命令コードを割り当てず、実プログラム上での使用頻度が低く、かつ、C P U 4 0 1 のデータ・演算処理用の資源に影響を与えることのない、既存命令のいずれかと同じ命令コードを重複して割り当てる点において、実施の形態 2 と異なる。

っている。

【0067】

実行領域判定回路 410 は、実行プログラムカウンタ値 s4018 から、図 7 に示したメモリ空間の領域区分に従い、現在実行されている命令の領域が特権領域、API 領域、ユーザ領域のいずれであるかを判定し、判定結果として実行領域判定信号 s410 を出力する。実行動作モード決定回路 411 は、実行領域判定信号 s410 の値に従い、実行動作モードを特権モード、API モード、ユーザモードのいずれかに決定する。決定結果は、実行動作モード決定信号 s411 として出力される。

【0068】

CPU 401 は、命令フェッチプログラムカウンタ値 s4015 または分岐先アドレス値 s4014 いずれかをメモリアクセス制御回路 4015 によって選択し、メモリアクセスアドレス信号 s4016 として出力する。

【0069】

分岐先領域判定回路 412 は、メモリアクセスアドレス信号 s4016 から、図 7 に示したメモリ空間の領域区分に従い、分岐先命令の領域が特権領域、API 領域、ユーザ領域のいずれであるかを判定し、判定結果として分岐先領域判定信号 s412 を出力する。分岐先動作モード決定回路 413 は、分岐先領域判定信号 s412 の値に従い、動作モードを特権モード、API モード、ユーザモードのいずれかに決定する。決定結果は、分岐先動作モード決定信号 s413 として出力される。

【0070】

動作モード変更検出回路 414 は、実行動作モード決定信号 s411 と分岐先動作モード決定信号 s413 から動作モードの変化を検出し、動作モード変更検出信号 s414 を出力する。

【0071】

不正分岐検出回路 409 は、動作モード変更検出信号 s414 と、命令フェッチデータ s407d に従い、以下の処理を行う。

【0072】

不正分岐検出回路 409 は、動作モード変更検出信号 s414 によって、ユーザプログラムから API プログラムへ、または、ユーザプログラムから特権プログラムへの実行の移行を伴う分岐命令が発生したことを判定した場合は、分岐先アドレスに格納されている命令コードを解読し、ユーザプログラムからの分岐を許可する分岐許可命令 (accept usr) でない場合は、割り込み要求として不正分岐検出割り込み要求信号 s409 を発生させる。

【0073】

不正分岐検出回路 409 は、動作モード変更検出信号 s414 によって、API プログラムから特権プログラムへの実行の移行を伴う分岐命令が発生したことを判定した場合は、分岐先アドレスに格納されている命令コードを解読し、ユーザプログラムからの分岐を許可する分岐許可命令 (accept usr) または API プログラムからの分岐を許可する分岐許可命令 (accept api) でない場合は、割り込み要求として不正分岐検出割り込み要求信号 s409 を発生させる。

【0074】

不正分岐検出回路 409 は、動作モード変更検出信号 414 によって、動作モードが変更しないと判定した場合、あるいは、動作モードが変更する場合であっても、その動作モードの変更が、ユーザプログラムから API プログラムへの変更、ユーザプログラムから特権プログラム、または API プログラムから特権プログラムへの変更のいずれでもないと判定した場合は、何も処理しない。

【0075】

分岐許可命令 (accept) は既存命令と同一の命令コードに割り当てられているため、命令解読部 4012 は既存のものを使用できる。また、CPU 401 内部の分岐許可命令 (accept) に対する処理は、割り当てられた既存命令と同一の実行処理内容、実行処理サイクルで実行される。

【0076】

以上により、動作モードの移行を伴う分岐命令が実行された際、分岐先アドレス上にその分岐命令の実行を許可する分岐許可命令が格納されていない場合は、不正分岐検出回路 409 が割り込み要求信号 s409 を出力するため、例えばフ

ラッシュメモリ 4 0 4 に外部から追加されたユーザプログラム等によって命令 ROM 4 0 2 に格納された特権プログラムが不正に実行されることを防ぎ、セキュリティを確保できる。

【 0 0 7 7 】

正当な処理の場合、実行を希望するプログラムが格納されているアドレスに対して直接分岐命令を実行できるので、動作モードの移行を分岐許可命令に割り当てられた既存命令 1 命令分と同一の実行処理サイクルで処理でき、リアルタイム性が向上する。また、CPU 4 0 1 に関しては既存のものを流用できるため設計容易性が高い。

【 0 0 7 8 】

(実施の形態 4)

図 4 は、実施の形態 4 にかかるプロセッサを用いた IC カードシステムを表すブロック図である。

【 0 0 7 9 】

本実施形態のプロセッサを用いた IC カードシステムは、図 4 に示すように、CPU 7 0 1 と、命令 ROM 7 0 2 と、RAM 7 0 3 と、フラッシュメモリ 7 0 4 と、外部 I / F 7 0 5 と、アンテナコイル 7 0 6 と、アドレスバス 7 0 7 a と、データバス 7 0 7 d と、割り込み制御回路 7 0 8 と、不正分岐検出回路 7 0 9 と、実行領域判定回路 7 1 0 と、実行動作モード決定回路 7 1 1 と、分岐先領域判定回路 7 1 2 と、分岐先動作モード決定回路 7 1 3 と、動作モード変更検出回路 7 1 4 と、分岐許可命令コード変換回路 7 1 5 とによって構成される。

【 0 0 8 0 】

更に、CPU 7 0 1 は、命令フェッチ部 7 0 1 1 と、命令解読部 7 0 1 2 と、命令実行部 7 0 1 3 と、プログラムカウンタ 7 0 1 4 と、メモリアクセス制御回路 7 0 1 5 とによって構成される。

【 0 0 8 1 】

CPU 7 0 1 は、命令 ROM 7 0 2 またはフラッシュメモリ 7 0 4 に格納された命令を読み出し実行していく。フラッシュメモリ 7 0 4 に対しては、アンテナコイル 7 0 6 および外部 I / F 7 0 5 を介して、外部からプログラムデータを追

加することが可能である。

【0082】

本実施形態のプロセッサを用いたメモリ空間の領域区分の概念図は、実施の形態1で説明した図7のとおりである。

【0083】

図3は、実施の形態4のプロセッサ用のプログラム概念図である。

【0084】

A P I 領域中の A P I プログラム 602 には、ユーザ領域中のユーザプログラム 603 から分岐命令 (j m p) によって A P I 領域中の A P I プログラム 602 に実行が移行する際に、A P I 領域中の分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令 (a c c e p t u s r) を記述する。

【0085】

特権領域中の特権プログラム 601 には、ユーザ領域中のユーザプログラム 603 から分岐命令 (j m p) によって特権領域中の特権プログラム 601 に実行が移行する際に、特権領域中の分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令 (a c c e p t u s r) を記述する。

【0086】

また特権領域中の特権プログラム 601 には、A P I 領域中の A P I プログラム 602 から分岐命令 (j m p) によって特権領域中の特権プログラム 601 に実行が移行する際に、特権領域中の分岐先アドレスが正当なアドレスかどうかを指定するための分岐許可命令 (a c c e p t a p i) を記述する。

【0087】

すなわち、本実施形態のプロセッサ用のプログラム記述は、前述の実施の形態3と同様である。ただし、本実施形態では、分岐許可命令 (a c c e p t) は、既存命令の命令コードと一致しない特別の命令コードを持つ。

【0088】

実行領域判定回路 710 は、実行プログラムカウンタ値 s 7018 から、図7に示したメモリ空間の領域区分に従い、現在実行されている命令の領域が特権領域、A P I 領域、ユーザ領域のいずれであることを判定し、判定結果として実行領

域判定信号 s 7 1 0 を出力する。実行動作モード決定回路 7 1 1 は、実行領域判定信号 s 7 1 0 の値に従い、実行動作モードを特権モード、A P I モード、ユーザモードのいずれかに決定する。決定結果は、実行動作モード決定信号 s 7 1 1 として出力される。

【0089】

C P U 7 0 1 は、命令フェッチプログラムカウンタ値 s 7 0 1 5 または分岐先アドレス値 s 7 0 1 4 いずれかをメモリアクセス制御回路 7 0 1 5 によって選択し、メモリアクセスアドレス信号 s 7 0 1 6 として出力する。

【0090】

分岐先領域判定回路 7 1 2 は、メモリアクセスアドレス信号 s 7 0 1 6 から、図 7 に示したメモリ空間の領域区分に従い、分岐先命令の領域が特権領域、A P I 領域、ユーザ領域のいずれであるかを判定し、判定結果として分岐先領域判定信号 s 7 1 2 を出力する。分岐先動作モード決定回路 7 1 3 は、分岐先領域判定信号 s 7 1 2 の値に従い、動作モードを特権モード、A P I モード、ユーザモードのいずれかに決定する。決定結果は、分岐先動作モード決定信号 s 7 1 3 として出力される。

【0091】

動作モード変更検出回路 7 1 4 は、実行動作モード決定信号 s 7 1 1 と分岐先動作モード決定信号 s 7 1 3 から動作モードの変化を検出し、動作モード変更検出信号 s 7 1 4 を出力する。

【0092】

不正分岐検出回路 7 0 9 は、動作モード変更検出信号 s 7 1 4 と、命令フェッチデータ s 7 0 7 d に従い、以下の処理を行う。

【0093】

不正分岐検出回路 7 0 9 は、動作モード変更検出信号 s 7 1 4 によって、ユーザプログラムから A P I プログラム、または、ユーザプログラムから特権プログラムへの実行の移行を伴う分岐命令が発生したことを判定した場合は、分岐先アドレスに格納されている命令コードを解読し、ユーザプログラムからの分岐を許可する分岐許可命令 (a c c e p t u s r) でない場合は、割り込み要求とし

て不正分岐検出割り込み要求信号 s 7 0 9 を発生させる。

【0094】

不正分岐検出回路 7 0 9 は、動作モード変更検出信号 s 7 1 4 によって、A P I プログラムから特権プログラムへの実行の移行を伴う分岐命令が発生したことを判定した場合は、分岐先アドレスに格納されている命令コードを解読し、ユーザプログラムからの分岐を許可する分岐許可命令 (a c c e p t u s r) または A P I プログラムからの分岐を許可する分岐許可命令 (a c c e p t a p i) でない場合は、割り込み要求として不正分岐検出割り込み要求信号 s 7 0 9 を発生させる。

【0095】

不正分岐検出回路 7 0 9 は、動作モード変更検出信号 7 1 4 によって、動作モードが変更しないと判定した場合、あるいは、動作モードが変更する場合であっても、その動作モードの変更が、ユーザプログラムから A P I プログラムへの変更、ユーザプログラムから特権プログラム、または A P I プログラムから特権プログラムへの変更のいずれでもないと判定した場合は、何も処理しない。

【0096】

分岐許可命令コード変換回路 7 1 5 は、命令フェッチデータ s 7 0 7 d が、ユーザプログラムからの分岐を許可する分岐許可命令 (a c c e p t u s r) の命令コードまたは A P I プログラムからの分岐を許可する分岐許可命令 (a c c e p t a p i) の命令コードと同一の場合は、ノーオペレーション命令の命令コードにデータ変換を行い、それ以外は何も処理せずに、C P U 7 0 1 に対し、命令フェッチデータ信号 s 7 0 1 1 を出力する。

【0097】

分岐許可命令 (a c c e p t) は、既存命令と同一の命令コードに割り当てられているため、命令解読部 7 0 1 2 は既存のものを使用できる。また、C P U 7 0 1 内部の分岐許可命令 (a c c e p t) に対する処理は、割り当てられた既存命令と同一の実行処理内容、実行処理サイクルで実行される。

【0098】

以上により、動作モードの移行を伴う分岐命令が実行された際、分岐先アドレ

ス上にその分岐命令の実行を許可する分岐許可命令が格納されていない場合は、不正分岐検出回路 709 が割り込み要求信号 s 709 を出力するため、例えばフラッシュメモリ 404 に外部から追加されたユーザプログラム等によって命令 ROM 402 に格納された特権プログラムが不正に実行されることを防ぎ、セキュリティを確保できる。

【0099】

正当な処理の場合、実行を希望するプログラムが格納されているアドレスに対して直接分岐命令を実行できるので、動作モードの移行を最短実行処理サイクルで処理でき、リアルタイム性が向上する。また、CPU 701 に関しては既存のものを流用できるため設計容易性が高い。

【0100】

なお、上述の実施の形態 1～4 では、不正分岐検出部、実行領域判定部、実行動作モード決定部等のそれぞれを別個独立した回路として形成したが、これらの各部ブロックをどのように実装するかは任意である。すなわち、例えば、実行領域判定部と実行動作モード決定部のような複数のブロックを一つの回路で実現した構成も、本発明の技術的範囲に属する。

【0101】

また、実施の形態 1～4 では、本発明のプロセッサを IC カードシステムに適用した例を示したが、本発明のプロセッサの用途はこれに限定されない。

【0102】

(実施の形態 5)

図 5 は、実施の形態 5 を用いたコンパイラ装置の構成およびコンパイルフローである。

【0103】

本実施形態にかかるコンパイラ 802 は、C 言語ソースコード 801 を入力してコンパイルし、アセンブラ 803 に変換する。

【0104】

C 言語ソースコード 801 は、ユーザ領域中に記述されたメイン関数 (main_1) 16011 と、特権領域中に記述された関数 16012 (function_a) と関数

16013 (function_b) によって構成されている。また、ユーザプログラムのメイン関数 (main_1) 16011 は、プログラム中で関数 16012 (function_a) および関数 16013 (function_b) を呼び出し使用する。

【0105】

コンパイラ 802 は、コンパイルを行う際に、C 言語ソースコード 801 中の関数が、それぞれ特権領域、ユーザ領域のいずれに記述されているか判定し、特権領域中に記述された関数を特権プログラムとして決定する。コンパイラ 802 は、コンパイルを実行する際に、特権プログラムのソースコードから生成されるアセンブラコードの先頭に、分岐許可命令 (accept) 16032, 16033 を挿入する。

【0106】

以上により、特権領域中のプログラムの開発を行う設計者は、C 言語によるプログラム記述方法を使用しても、コンパイル時に分岐許可命令 (accept) が自動挿入され、動作モードの移行を伴う分岐が発生した際の命令実行に対するセキュリティを確保できる。

【0107】

【発明の効果】

以上のように、ユーザプログラムから特権プログラムまたは API プログラム中のアドレスに対して分岐命令が実行された際、分岐先アドレス上に分岐許可命令が格納されていない場合は不正分岐検出部が割り込み要求信号を出力するため、ユーザプログラムによって特権プログラムが不正に実行されることを防ぎセキュリティを確保できる。またユーザプログラム上から特権プログラムまたは API プログラムを正当に実行する際、ユーザプログラム上で実行を希望する特権プログラムまたは API プログラムが格納されているアドレスに対して直接分岐命令を実行することができるため、動作モードの移行に伴う処理時間が削減されリアルタイム性が向上する。

【図面の簡単な説明】

【図 1】 実施の形態 1、実施の形態 2、実施の形態 3 におけるプロセッサ回路構成

【図2】 実施の形態1におけるプログラム概念図

【図3】 実施の形態2、実施の形態3、実施の形態4におけるプログラム概念図

【図4】 実施の形態2におけるプロセッサ回路構成

【図5】 実施の形態5におけるコンパイラ装置の構成

【図6】 従来のプロセッサ回路構成

【図7】 アドレス空間の領域区分

【図8】 従来のプログラム概念図

【符号の説明】

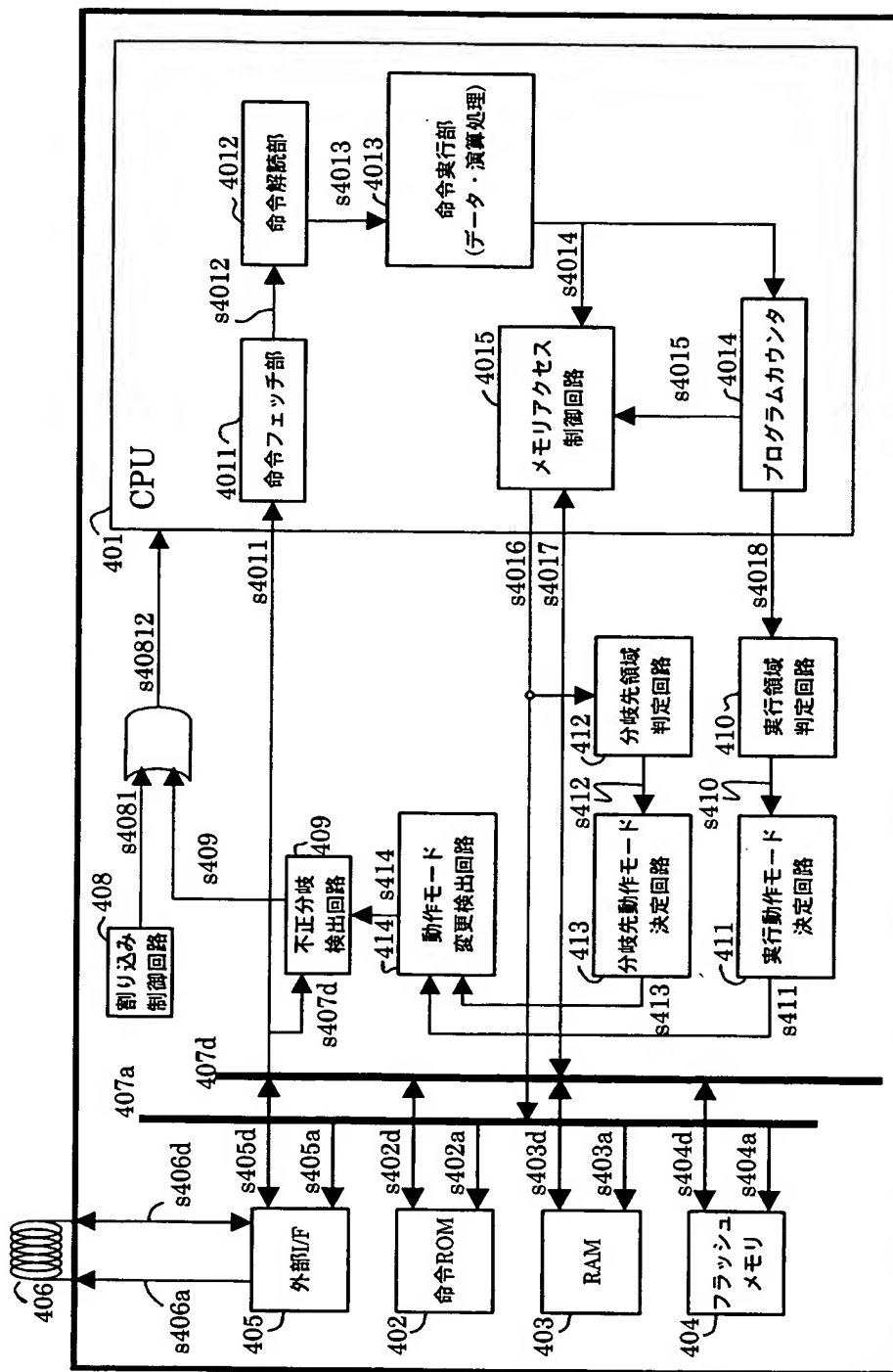
200	全論理アドレス空間
211	命令ROM空間特権領域
212	命令ROM空間API領域
221	RAM空間特権領域
222	RAM空間API領域
223	RAM空間ユーザ領域
231	フラッシュ空間ユーザ領域
241	外部I/F空間ユーザ領域
301	特権領域
302	ユーザ領域
401, 701	CPU
4011, 7011	命令フェッチ部
4012, 7012	命令解読部
4013, 7013	命令実行部
4014, 7014	プログラムカウンタ
4015, 7015	メモリアクセス制御回路
402, 702	命令ROM
403, 703	RAM
404, 704	フラッシュメモリ
405, 705	外部I/F

4 0 6, 7 0 6	アンテナコイル
4 0 7 a, 7 0 7 a	アドレスバス
4 0 7 d, 7 0 7 d	データバス
4 0 8, 7 0 8	割り込み制御回路
4 0 9, 7 0 9	不正分岐検出回路
4 1 0, 7 1 0	実行領域判定回路
4 1 1, 7 1 1	実行動作モード決定回路
4 1 2, 7 1 2	分岐先領域判定回路
4 1 3, 7 1 3	分岐先動作モード決定回路
4 1 4, 7 1 4	動作モード変更検出回路
5 0 1	特権領域
5 0 2	A P I 領域
5 0 3	ユーザ領域
6 0 1	特権領域
6 0 2	A P I 領域
6 0 3	ユーザ領域
7 1 5	分岐許可命令コード変換回路
8 0 1	C 言語ソースコード
8 0 2	コンパイラ
8 0 3	アセンブラソースファイル

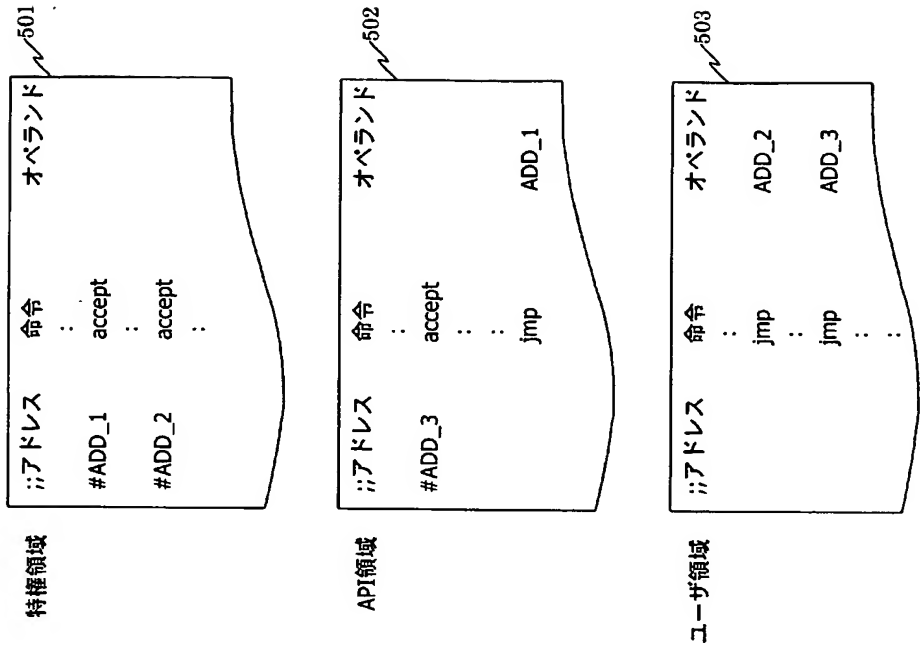
【書類名】

図面

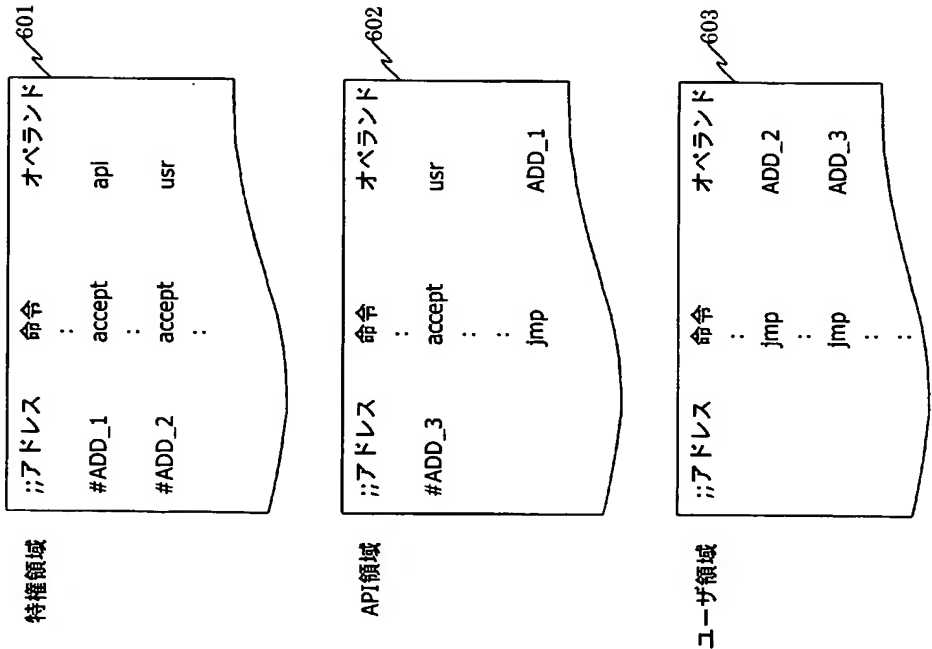
【図 1】



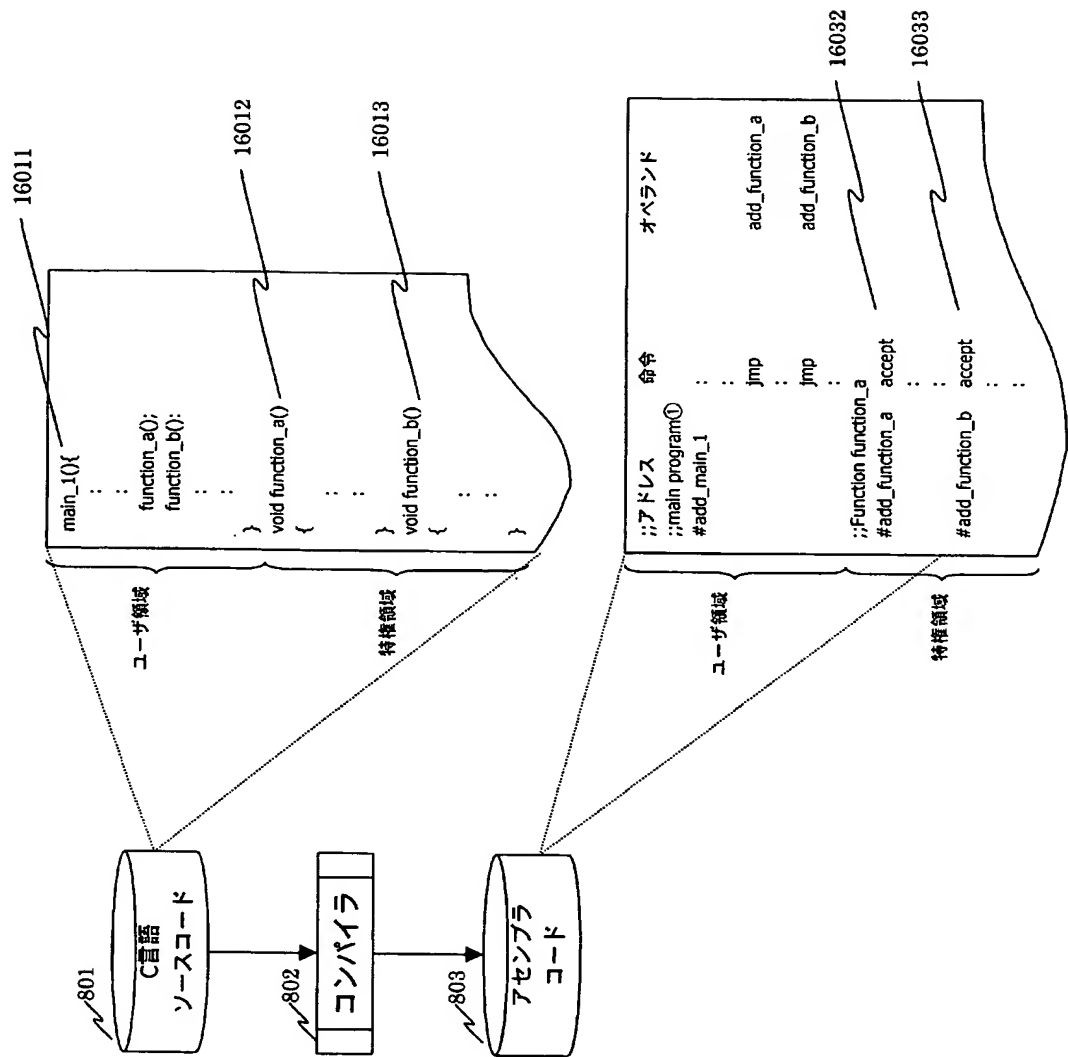
【図 2】



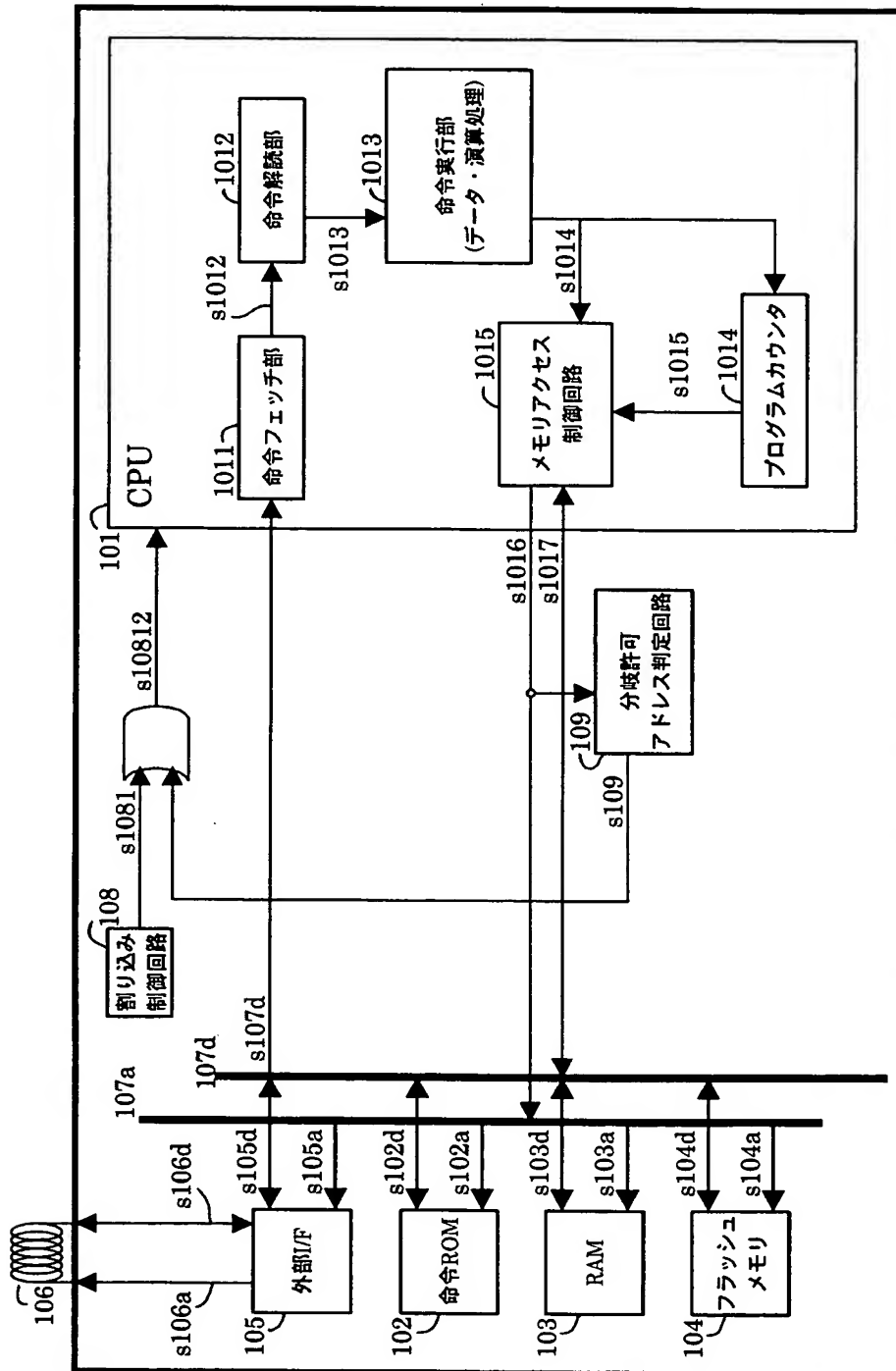
【図 3】



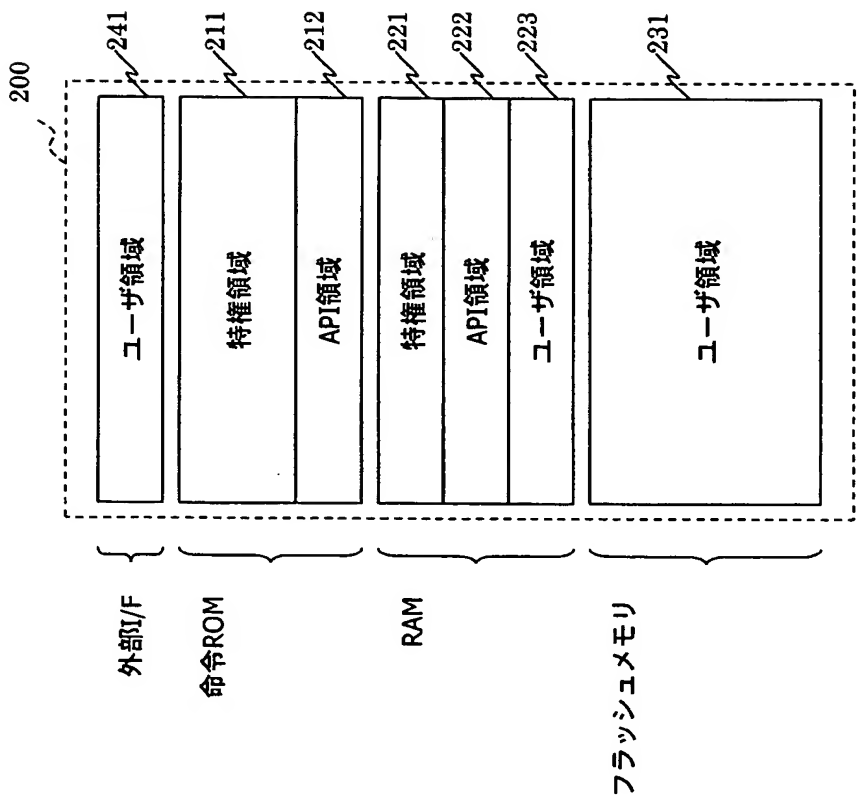
【図 5】



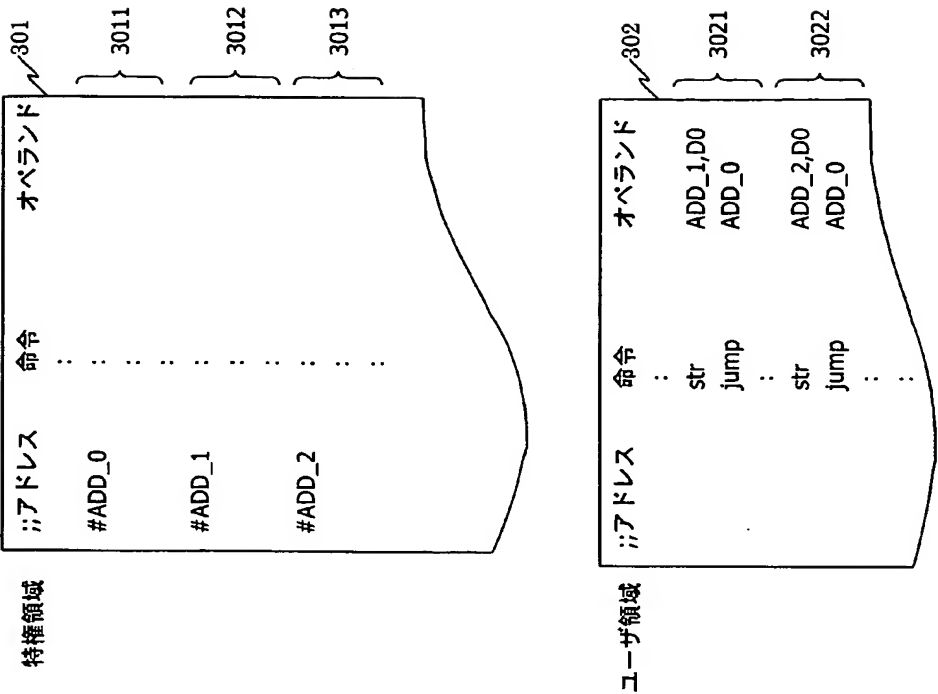
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 ユーザプログラムによって特権プログラムが不正に実行されることを防ぎセキュリティを確保すると共に、ユーザプログラムから特権プログラムへの正当な分岐の場合のリアルタイム性を向上させるプロセッサを提供する。

【解決手段】 CPU 4 0 1 と、プログラムを格納するためのフラッシュメモリ 4 0 4 とを備えたプロセッサにおいて、フラッシュメモリ 4 0 4 に格納されているプログラムによって、動作モードを異なる動作モードへ変更する分岐命令が実行された際、不正分岐検出回路 4 0 9 が、分岐先アドレスに分岐許可命令が存在するか否かを判断し、前記分岐許可命令が存在しない場合は割り込み要求を出力することにより、ユーザプログラムによって特権プログラムが不正に実行されることを防止する。

【選択図】 図 1

特願 2 0 0 3 - 0 4 6 4 8 4

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1 . 変 更 年 月 日

1 9 9 0 年 8 月 2 8 日

[変 更 理 由]

新 規 登 録

住 所

大 阪 府 門 真 市 大 字 門 真 1 0 0 6 番 地

氏 名

松 下 電 器 産 業 株 式 会 社